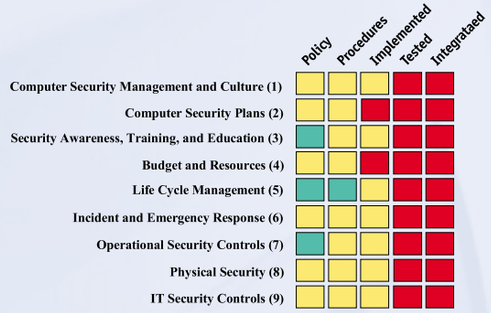
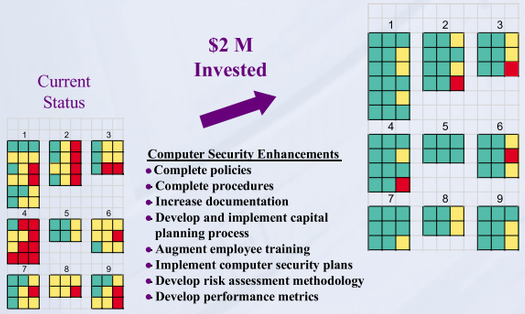
IT SECURITY STATUS

- Each review area examined with regard to:
  - Existence of policy
  - Existence of procedures
  - Whether or not implemented
  - Whether or not tested
  - Whether or not integrated
- Each area identified as:
  - Compliant
  - Partially compliant
  - Not compliant

SAMPLE OVERVIEW OF AGENCY STATUS



SAMPLE CHANGE IN COMPUTER SECURITY POSTURE AFTER $2 MILLION ACTION PLAN



"NIST CSEAT Team has just finished their review of our Information Security program and given us the draft report. They have done a great job for us. The report is a first-rate product and gives us a very practical guide on how best to apply our limited resources to fix our shortfalls."

"Of all the reviews and audits we have done on us or against us, this is the most useful."

From communication between agency CIO and OMB

"Each review will produce high-level findings, a "sanity check" of how well personnel understand policies, and report with prioritized recommendations."

Government Computer News Daily Update, August 1, 2001

Perform Agency Review

Identify Computer Security Needs

Computer Security Expert Assist Team
CSEAT

Develop Relevant Guidelines

Provide Agency With Action Plan

A federal agency can request a review by emailing the CSEAT:

cseat@nist.gov
http://cseat.nist.gov/

or contact the Director of the Computer Security Expert Assist Team, Joan Hash at 301-975-3357

NIST CENTENNIAL 1901-2001

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NIST'S INFORMATION TECHNOLOGY LABORATORY

Guide to the

Computer Security Expert Assist Team
CSEAT

Computer Security Program

Background

The Computer Security Expert Assist Team (CSEAT) was established at the National Institute of Standards and Technology (NIST) to improve federal Critical Infrastructure Protection (CIP) planning and implementation efforts by assisting governmental entities in improving the security of their information and cyber assets. The CSEAT accomplishes this by performing a review of an agency's computer security program. The review is based upon a combination of proven techniques and best practices and results in an action plan that provides a federal agency with a business case based roadmap to cost-effectively enhance the protection of their information system assets.

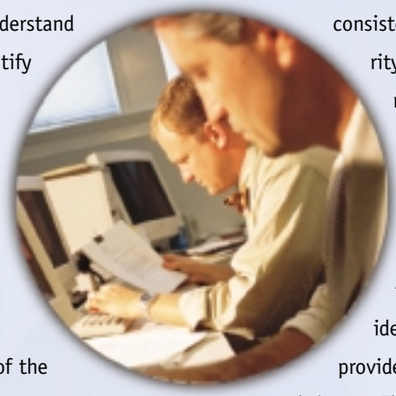
Each agency must implement and maintain an active information technology security program that adequately secures agency information assets. An agency's IT security program must: **1)** assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and **2)** protect information commensurate with the level of risk and magnitude of harm resulting from the information's loss, misuse, unauthorized access, or modification.

Purpose

The CSEAT has three primary purposes:

1. To assist agencies in improving the security of federal IT systems,
2. To help reduce disruption of critical federal systems/services, and
3. To improve federal agency CIP planning and implementation efforts.

The CSEAT also helps Federal agencies understand how to protect information systems, identify and fix existing vulnerabilities, and prepare for future security threats. The CSEAT also facilitates exchange of best security practices among government agencies and between the government and private sector.



The initial CSEAT approach is comprised of the following two types of reviews:

- Reviewing agency automated information security programs (computer security for the organization) as requested by a Federal agency, and
- Reviewing existing and planned high-risk IT systems as requested by OMB and a Federal agency.

Both of these types of reviews are instrumental in identifying agencies computer security needs. Once these needs are identified, the CSEAT can develop best practices and guidelines relevant to existing federal computer security needs.

CSEAT Security Program Review Approach

CSEAT provides an independent review of an agency's IT security program. The CSEAT review, which is not an audit or an inspection, begins with an assessment of the maturity of the agency's IT security program. This includes the agency's IT security policies, procedures, and security controls implementation and integration across all business areas. The CSEAT review provides a consistent and comparable approach to IT security through consistent application of security control objectives and IT security effectiveness criteria. CSEAT performs a comparable review of the agency's organizational structure, culture, and business mission. After the assessment is performed, the CSEAT documents issues identified during the assessment phase and provides corrective actions associated with each issue. These corrective actions are then provided as a prioritized action plan for the agency to use to improve their computer security program.

The CSEAT does not establish new security requirements. The CSEAT security control objectives are abstracted directly from long-standing requirements found in federal government regulations, statutes, policies, and guidance on security.

CSEAT Review Report and Action Plan

The CSEAT review report is organized into nine subsections, each of which were derived from a combination of NIST 800-26 Self-Assessment Guide for Information Technology Systems as enhanced by other criteria from requirements and guidance such as NIST 800-18 Guide for Developing Security Plans for Information Technology Systems, OMB Circular A-130 (Management of Federal Information Resources), and OMB M-01-24 Reporting Instructions for the Government Information Security Reform Act. The critical areas are supplemented by additional evaluation criteria derived from a combination of best commercial and governmental practices, industry standards, and other regulatory requirements.

CSEAT review reports provide recommendations relative to the agency's:

- Cyber security culture including policies and procedures, and roles and responsibilities,
- System security plans and risk assessment/analysis,
- IT security personnel, user, and management training and awareness programs,
- Budget and resources dedicated to IT security,
- IT life cycle methodology and incorporation of IT security,
- Incident and emergency response,
- Operations including authorized processing,
- Physical security, and
- IT security access controls.

The resulting action plan is weighted to provide the agency the greatest improvements most cost effectively. The corrective actions CSEAT identifies include the time frame for implementation and the projected resource impact. The action plan can readily be used to develop scopes of work for quick "bootstrapping" of the cyber security program.